



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/523,720

02/07/2005

Toshihiko Fukuoka

71971-132

1073

20277 7590 05/22/2008
MCDERMOTT WILL & EMERY LLP
600 13TH STREET, N.W.
WASHINGTON, DC 20005-3096

EXAMINER

SCHWARTZ, DARREN B

ART UNIT

PAPER NUMBER

2135

MAIL DATE

DELIVERY MODE

05/22/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/523,720	Applicant(s) FUKUOKA ET AL.	
	Examiner DARREN SCHWARTZ	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 February 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 21-37 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 21-37 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 February 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>02-07-05 08-18-05</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 34-37 are rejected under 35 U.S.C. 102(b) as being anticipated by Hawe et al (U.S. Pat 5070528 A), hereinafter referred to as Hawe.

Re claim 34: Hawe teaches a transmission/reception apparatus comprising: a downstream PHY section for converting a received signal into data and outputting the converted data; a downstream data processing section for separating downstream data and key data from the received data and outputting the resultant data; a first encryption/decryption device for decrypting the downstream data using the key data and outputting the decrypted data; a storage section for storing the decrypted downstream data; a second encryption/decryption device for encrypting upstream data read from the storage section and outputting the encrypted data; an upstream data processing section for adding key data used for the encryption to the encrypted upstream data and outputting the resultant data; and an upstream PHY section for converting the data output from the upstream data processing section into a signal and transmitting the signal (Fig 2, all elts; col 8, line 61 – col 9, line 40),

wherein both the first and second encryption/decryption devices comprise: a data structure analysis block for receiving the downstream data including encrypted data or the upstream data including data to be encrypted, analyzing the structure of the data

and outputting information related to encryption as control data, the data structure analysis block also outputting the encrypted data or the data to be encrypted as processing block input data (col 9, lines 5-42; col 13, lines 22-41; col 14, lines 36-61);

a data control block for outputting an encryption/decryption switch signal indicating which one of encryption and decryption should be performed, and a mode selection signal indicating in which mode the processing block input data should be processed, according to the control data (col 10, lines 34-44; col 13, lines 22-41; col 14, lines 36-61);

and a shared processing block for performing encryption or decryption for the processing block input data according to the encryption/decryption switch signal, and outputting encrypted result or decrypted result, wherein the shared processing block is configured to have the ability to perform encryption and decryption in either of the CBC mode and the CFB mode by performing ECB processing using input key data, and performs encryption or decryption in the mode indicated by the mode selection signal (col 19, line 7 – col 20, line 44).

Re claims 35, 36 and 37: Hawe teaches an encryption/decryption method comprising: a data structure analysis step of analyzing the structure of encrypted data or data to be encrypted to determine information related to encryption as control data, and also determining the encrypted data or the data to be encrypted as processing block input data (col 9, lines 5-42; col 13, lines 22-41; col 14, lines 36-61);

a data control step of determining an encryption/decryption switch signal indicating which one of encryption and decryption should be performed, and mode selection data indicating in which mode the processing block input data should be

processed, according to the control data (col 10, lines 34-44; col 13, lines 22-41; col 14, lines 36-61); and

a shared processing step of performing encryption or decryption for the processing block input data according to the encryption/decryption switch signal to determine encrypted result or decrypted result, wherein the shared processing step includes having the ability to perform encryption and decryption in either of the CBC mode and the CFB mode by performing ECB processing using key data, and performing encryption or decryption in the mode indicated by the mode selection data (col 19, line 7 – col 20, line 44).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 21-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hawe et al (U.S. Pat 5070528 A), hereinafter referred to as Hawe, in view of Hasebe et al (JP 2000-075785 A), hereinafter referred to as Hasebe (a translated copy of this document has been provided with this office action).

Re claims 21, 32, 33: Hawe teaches an encryption/decryption device comprising:

a data structure analysis block for receiving encrypted data or data to be encrypted (Fig 2, all elts), analyzing the structure of the data and outputting information related to encryption as control data, the data structure analysis block also outputting

the encrypted data or the data to be encrypted as processing block input data (col 9, lines 5-42; col 13, lines 22-41; col 14, lines 36-61);

a data control block for outputting an encryption/decryption switch signal indicating which one of encryption and decryption should be performed, and a mode selection signal indicating in which mode the processing block input data should be processed, according to the control data (col 10, lines 34-44; col 13, lines 22-41; col 14, lines 36-61); and

a shared processing block configured to have the ability to perform encryption and decryption in either of the Cipher Block Chaining (CBC) mode and the Cipher Feedback (CFB) mode by performing Electronic Code Book (ECB) processing using input key data, the shared processing block performing encryption or decryption according to the encryption/decryption switch signal for the processing block input data in the mode indicated by the mode selection signal, and outputting encrypted result or decrypted result (col 19, line 7 – col 20, line 44),

However, Hasebe teaches the shared processing block comprises: an ECB processor for performing the ECB processing and outputting the result as cipher-processed data; a first selector for selecting one of the processing block input data and the cipher-processed data according to the encryption/decryption switch signal and the mode selection signal, and outputting the selected data; a delay device for delaying the processing block input data and the cipher-processed data received as inputs and outputting the delayed data; a second selector for selecting one of the processing block input data, initial vector data, and the delayed processing block input data and the delayed cipher-processed data output from the delay device according to the

encryption/decryption switch signal and the mode selection signal, and outputting the selected data; an XOR operator for computing XOR of the output of the first selector and the output of the second selector and outputting the computed result; a third selector for selecting one of the processing block input data, the output of the XOR operator, the delayed processing block input data and the delayed cipher-processed data according to the encryption/decryption switch signal and the mode selection signal, and outputting the selected data; a bit mask device for masking part of the key data as required according to the mode selection signal and outputting the result as mode-adaptive key data; and a fourth selector for selecting one of the cipher-processed data and the output of the XOR operator according to the encryption/decryption switch signal and the mode selection signal, and outputting the selected data as the encrypted result or the decrypted result, and the ECB processor performs either encryption or decryption as the ECB processing for the output of the third selector using the mode-adaptive key data according to the encryption/decryption switch signal and the mode selection signal, and outputs the result as the cipher-processed data (drawing 27; selectors 22, 23, 27, 31, 32, 35, 41, 46).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of the Hawe reference with the teachings of the Hasebe for the purpose of providing more cipher options to the sending and receiving parties while using fast and secure symmetric systems.

Re claim 22: Hawe in view of Hasebe teaches the data structure analysis block analyzes a header of the encrypted data to draw out a Media Access Control (MAC) structure from the encrypted data based on information in the header, and if an

extension header exists in the MAC structure and the extension header indicates that the encrypted data has been encrypted, the data structure analysis block outputs information related to encryption included in the extension header as the control data, and also removes the extension header from the MAC structure data and outputs the result as the processing block input data (Hawe: col 7, lines 2-10; col 9, lines 5-40; col 9, line 65 - col 10, line 33).

Re claim 23: Hawe in view of Hasebe teaches the data control block outputs a signal indicating in which mode, the CBC mode or the CFB mode, the processing block input data should be processed and in which key data length mode the data should be processed, as the mode selection signal, according to the control data (Hawe: col 6, lines 44-54; col 7, lines 2-10; col 13, lines 22-41; Hasebe: claims 1, 9, 14 and 15).

Re claim 24: Hawe in view of Hasebe teaches the bit mask device outputs the key data as it is if the mode selection signal indicates a 56-bit key mode, or otherwise masks unnecessary bits and outputs the resultant data, as the mode-adaptive key data (Hasebe: ¶8, ¶25, ¶27, ¶55-56 and ¶64).

Re claim 25: Hawe in view of Hasebe teaches the first selector selects the processing block input data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CBC mode, or otherwise selects the cipher-processed data, and outputs the selected data (Hawe: col 6, lines 44-54; col 7, lines 2-10; col 13, lines 22-41; Hasebe: drawing 27; selectors 22, 23, 27, 31, 32, 35, 41, 46).

Re claim 26: Hawe in view of Hasebe teaches the second selector selects the initial vector data at start of processing and thereafter selects the delayed cipher-

processed data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CBC mode, and outputs the selected data, selects the initial vector data at start of processing and thereafter selects the processing block input data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CFB mode, and outputs the selected data, selects the initial vector data at start of processing and thereafter selects the delayed processing block input data if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CBC mode, and outputs the selected data, or selects the initial vector data at start of processing and thereafter selects the processing block input data if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CFB mode, and outputs the selected data (Hawe: col 6, lines 44-54; col 7, lines 2-10; col 13, lines 22-41; Hasebe: drawing 27; selectors 22, 23, 27, 31, 32, 35, 41, 46; ¶7; ¶9, ¶11-12, ¶14).

Re claim 27: Hawe in view of Hasebe teaches the third selector selects the output of the XOR operator if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CBC mode, and outputs the selected data, selects the processing block input data at start of processing and thereafter selects the delayed cipher-processed data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CFB mode, and outputs the selected data, selects the processing block input data if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CBC mode, and outputs the selected data, or selects the processing block input data at start of processing and thereafter selects the delayed processing block

input data if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CFB mode, and outputs the selected data (Hawe: col 6, lines 44-54; col 7 , lines 2-10; col 13, lines 22-41; Hasebe: drawing 27; selectors 22, 23, 27, 31, 32, 35, 41, 46; ¶20).

Re claim 28: Hawe in view of Hasebe teaches the fourth selector selects the cipher-processed data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CBC mode, and outputs the selected data, selects the output of the XOR operator if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CFB mode, and outputs the selected data, or selects the output of the XOR operator if the encryption/decryption switch signal indicates decryption, and outputs the selected data (Hawe: col 6, lines 44-54; col 7 , lines 2-10; col 13, lines 22-41; Hasebe: drawing 27; selectors 22, 23, 27, 31, 32, 35, 41, 46; ¶14; ¶43; ¶61).

Re claim 29: Hawe in view of Hasebe teaches the ECB processor performs encryption if the encryption/decryption switch signal indicates encryption, performs decryption if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CBC mode, or performs encryption if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CFB mode (Hawe: col 6, lines 44-54; col 7 , lines 2-10; col 13, lines 22-41; col 19, line 7 – col 20, line 44),

Re claim 30: Hawe in view of Hasebe teach all the limitations of claim 30 as discussed per claim 1. Additionally, it is known in the art that once processing in the shared processing block is performed for the encrypted data or the data to be encrypted

for a predetermined number of times, the output selector selects the output of the shared processing block. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have several rounds of encryption/decryption for the purpose of having a more secure algorithm; such technique is used in DES, 3DES and the like.

Re claim 31: The combination of Hawe, Hasebe and common knowledge in the art of symmetric ciphers teaches the predetermined number of times is three times. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have several rounds of encryption/decryption for the purpose of having a more secure algorithm; such technique is used in DES, 3DES and the like.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

JP 2001-177518 (a translated copy of this document has been provided with this office action)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 8am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2135
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135